SAND2015-2716R

SCENARIO ANALYSIS GUIDE

OUTLINE OF GUIDANCE FOR DEVELOPMENT OF SABOTAGE SCENARIOS

Sandia National Laboratories, NA-24 and NRA

Date Prepared: March 30, 2015

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Contents

Figures

No table of figures entries found.

Background

Pursuant to a request from Japan Nuclear Regulatory Authority (NRA) to collaborate with the United States Department of Energy (DOE) in efforts to exchange technical information in physical protection topics relating to the protection of nuclear material and facilities. Currently, there is a Project Action Sheet (PAS) in collaboration between NRA and DOE in implementing a collaboration study that consist of technical elements for development of sabotage scenarios for nuclear power plants (NPP).

The purpose for the collaboration study is pursuant to the newly published NNS-13 INFCIRC/225/Revision 5 with recommendations playing an important role in designing a physical protection system against sabotage. These recommendations state:

- 5.9. Using the threat assessment or design basis threat, the operator — in cooperation with the State's competent authority — should define credible scenarios by which adversaries could carry out sabotage of nuclear facilities and nuclear material.

- 5.10. When defining scenarios, the operator should consider the location of the nuclear facility and all nuclear material and other radioactive material, including radioactive waste, especially those at the same location inside a nuclear facility.

- 5.11. Sabotage scenarios should consider external and/or insider adversaries who attempt to disperse nuclear material or other radioactive material or to damage or interfere with equipment, systems, structures, components or devices, including possible stand-off attack, consistent with the State's threat assessment or design basis threat.

- 5.12. The operator should design a physical protection system that is effective against the defined sabotage scenarios and complies with the required level of protection for the nuclear facility and nuclear material.

- 5.52. The State should ensure that joint exercises, which simultaneously test emergency and contingency plans and actions, are regularly carried out in order to assess and validate the adequacy of the interfaces and response coordination of emergency and security organizations involved in responding to various scenarios, and should have a method for incorporating lessons learned to improve both management systems.

- 6.68. The State should ensure that joint exercises, which simultaneously test emergency and contingency plans and actions for transport of nuclear material are regularly carried out in order to assess and validate the adequacy of the interfaces and response coordination of emergency and security organizations involved in responding to various scenarios, and should have a method for incorporating lessons learned to improve both management systems.

NRA's primary objective to this study is to develop practical guidance for creating adversary attack scenarios dependent upon the threat assessment and Design Basis Threat (DBT). These adversary attack scenarios, in turn, can be used to design and evaluate the effectiveness of the physical protection system during performance testing exercises.

Physical Security Methodology

Prior to developing sabotage scenarios for nuclear power plants (NPP) a thorough and comprehensive review of the design and analysis of physical protection systems (PPS) for NPP facilities is necessary. The older NPP fleets do not have as much as an opportunity than the newer NPP designs as they can leverage passive safety and security features to design a cost effective integrated PPS design. Once a PPS is designed, conducting a thorough analysis will provide the Licensees confidence in determining the appropriate level of protection required for these types of reactors.

The design of an effective PPS includes identification of the PPS objectives, establishing the facility design, providing an initial design of a PPS, evaluation of the design, and a redesign or refinement of the system (if the system does not meet required protection objectives).

This is a methodological approach in which design and analysis of physical security is conducted in an integrated fashion where all components of detection, delay, and response are properly weighted according to their contributions to the PPS as a whole. This approach can assist in minimizing the potential for wasting valuable resources on unnecessary protection while at the same time maximizing protection to a facility.

For a more detailed, in-depth presentation of this process (i.e. design and evaluation of a PPS) see The Design and Evaluation of Physical Protection Systems by Mary Lynn Garcia [1]. This book incorporates knowledge from more than 30 years of PPS design and evaluation activities at Sandia National Laboratories. Figure 1 is a pictorial representation of this process.

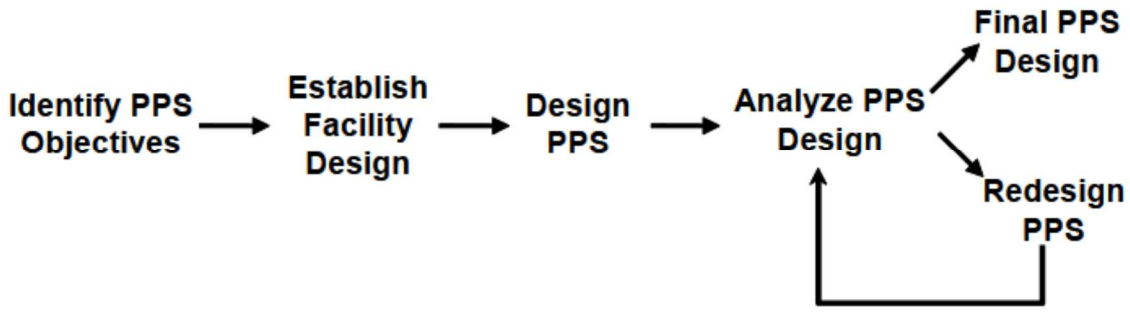

Figure 1: High Level description of a PPS design and evaluation process

When all physical protection objectives for the facility are identified from applicable regulations, a facility design is required along with identifying all known targets and hazards. Both qualitative and quantitative analyses such as Probabilistic Risk Assessments (PRA), Vital Area Identification (VAI), and Target Analysis (TA), be effectively utilized to identify targets or hazards while a Vulnerability Assessment (VA) can determine system effectiveness. Figure 2 is a pictorial representation of this process.

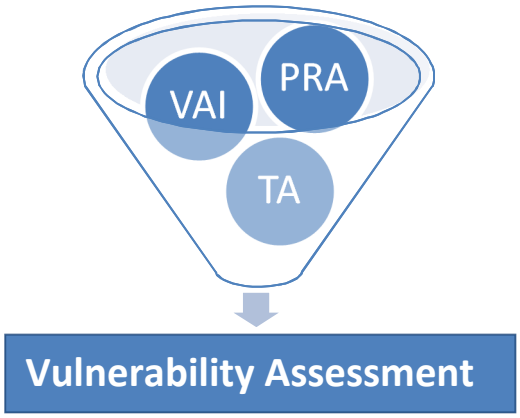

Figure 2: High Level description of NPP Analyses

Probabilistic Risk Assessment

For NPPs, the hazardous material of primary concern is the radioactive material contained in the reactor core and spent fuel storage locations (e.g. spent fuel pool). The primary safety concerns are accidents that can lead to reactivity insertion or disrupt the cooling of the material in these areas. Given the complex nature of a reactor and the potential for substantial consequences resulting from accidents, a PRA is typically employed. These accident sequences represent specific paths through the event trees that are used in a PRA. The information generated from the PRA is one of the necessary inputs to ensuring that security understands what must be protected from a safety related point of view.

Vital Area Identification

Security related target identification is a process of identifying specific safety operations and safeguards related areas or components that must be protected to prevent undesirable consequences. Given the complex nature of a reactor, one technique that may be employed to identify the security related targets is to use logic diagrams to identify vital areas. Vital Area Identification is a structured approach based on using fault trees from a PRA (i.e. logic diagrams) to identify the areas containing structures, systems, and components that, if destroyed or damaged by sabotage, result in the release of sufficient radioactive material such that the undesired safety related consequences occurs. This technique can be

modified to include the identification of areas that contain operations and safeguards related targets.

Target Sets and Target Analysis

The target sets are the sets of areas derived from the VAI that an adversary must access in order to commit sabotage. All areas in a specific target set must be accessed by an adversary to commit sabotage. Thus, the target sets answer the question of what must be attacked in order to sabotage the plant. The target analysis goes one step beyond the development of target sets by identifying the systems being disabled or the malicious initiating events being accomplished in each target area.

Vulnerability Assessment

The evaluation of an existing or proposed Physical Protection System (PPS) requires a methodical approach in which the ability of the security system to meet defined protection objectives is measured. Without this kind of careful assessment, valuable resources might be wasted on unnecessary protection or, worse yet, fail to provide adequate protection of warheads against a theft attack by the defined threat. The Vulnerability Assessment (VA) methodology was developed to implement performance-based physical security concepts at nuclear sites and facilities. **Figure** 3 is the flow diagram for the VA process.

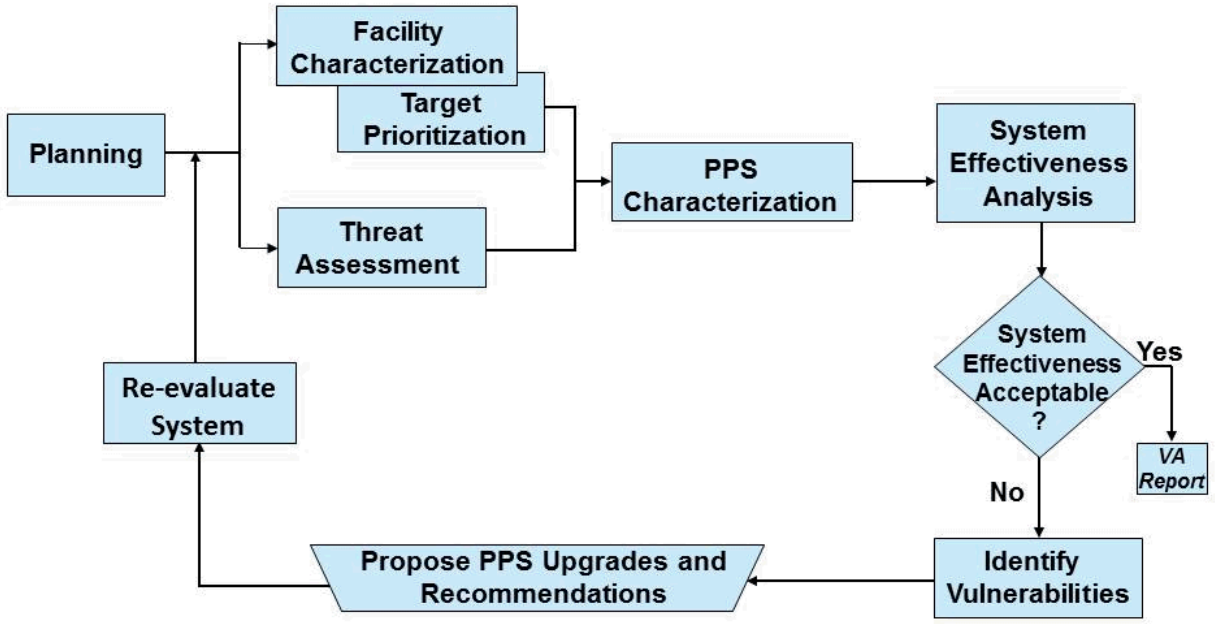

Figure 3. Process Flow Diagram for Vulnerability Assessment

The VA methodology consists of the following 12 steps:

- **Step 1. Identify the Vulnerability Analysis Team**. An effective VA requires a highly trained team with extensive knowledge and experience in physical protection and vulnerability analysis. The team requires (1) a project lead that can manage the entire VA process and ensure the analysis and results are correct and (2) specialized experts in the fields of detection, assessment, delay, response forces, analysis, and cyber security.

- **Step 2. Plan the VA.** Once the team is assembled, the project lead develops a project plan that outlines how the VA will be conducted. The project lead identifies team members' roles and responsibilities, develops the VA schedule, and gathers and distributes preliminary data and information to prepare for the facility characterization survey. Several project team meetings are conducted prior to the team's departure to the facility.

- **Step 3. Define the Threat**. Understanding the capabilities and attributes associated with the defined threat is vital to the design and/or upgrade of a PPS. Initially a broad threat spectrum is categorized into a specific subset of adversary unit size, skills, tactics, weapons, and capabilities, and forms the basis for designing the PPS. This subset is known as the Design Basis Threat (DBT).

- **Step 4. Characterize the Facility**. This process involves identifying and understanding the overall facility mission, nuclear operations and processes, company or state legal issues, and the physical conditions of the facility. All information and data collected is used to fully understand what must be protected (targets), from whom (threat), and to what performance level. Interviews are conducted at the facility to understand all aspects of the site and its operations. Physical protection and cyber security specialists conduct thorough site surveys to collect site data on essential PPS and cyber security elements.

- **Step 5. Identify and Prioritize Targets**. Target analysis involves identifying nuclear materials, items, and facilities at the site that must be protected to ensure a high level of system effectiveness against the DBT. These nuclear targets, processes, and operations are identified during the facility characterization phase as potential adversary targets and then prioritized based on their consequence category (e.g., Cat-1, Cat-2, Cat-3). Numerical consequence values (0 to 1) are then assigned to each target based on the resulting consequence level due to theft or sabotage of target.

- **Step 6. Define the PPS**. A detailed PPS characterization includes identifying facility security elements that provide detection, assessment, delay, and response capabilities. A thorough on-site survey allows security specialists to identify all protection elements and collect performance data for each component and the system as a whole. Performance-based data for identified security elements are incorporated into an Analytic System and Software for Evaluating Safeguards and Security (ASSESS) computer model of the facility. If performance-based data cannot be collected at the site, then database values from accepted and validated field tests and subject matter expert judgments are used to generate measures for the security elements.

- **Step 7. Conduct Probability of Interruption Analysis.** The site data collected and assumptions agreed to in Steps 4 and 6 (Facility and PPS Characterization) are used to construct models of all credible pathways from outside the facility perimeter to the targets of concern. ASSESS is used to construct an Adversary Sequence Diagram (ASD), which is a functional representation of the PPS at the facility and describes specific protection elements at the facility. Once the ASD is created and populated with site data, ASSESS is used to mathematically calculate the probabilities of interruption for each path (accumulated probabilities of assessed detection and delay times along the pathway), and the results are used to determine the most vulnerable adversary paths. The software default database values are from actual performance tests conducted to determine sensor probabilities of detection and barrier delay times as functions of adversary defeat techniques and tactics. These paths are subsequently reviewed to confirm credibility of detection probabilities and delay times. Any modification made to default values are based on site-specific performance tested data and/or subject matter expert (SME) engineering judgment. The justifications for modifications to default values are documented.

  Worst-case scenarios are developed by combining the most vulnerable paths with the facility's planned system response to an attack by the DBT. Detection probabilities and path delays are reviewed and modified, if necessary, to validate credibility and reflect real-world conditions. All potential and credible attack options are studied to ensure that worse-case attacks and other serious options that need to be protected against are identified. For the analysis, attack scenarios are described step-by-step, including when the adversary is detected, all adversary task times, and when the response force assesses and communicates the intrusion and interrupts the adversary's actions. These scenarios are used to estimate probability of neutralization.

- **Step 8. Conduct Probability of Neutralization Analysis**. Neutralization analysis provides information about how effective the facility's response force will be at neutralizing the threat using the identified worst-case scenarios. Conducting an actual attack at a facility is generally not possible; therefore, simulations are used to predict the probability of neutralizing violent adversaries after interrupting them. Although it is difficult to accurately model armed conflict between small forces, careful use of appropriate tools and methods can lead to results that indicate the likely performance of the response force if attacked (as defined by the DBT). These tools are used to estimate the likelihood that a response force will win against an attacking threat before it accomplishes its objective (theft or sabotage).

  Tabletop and neutralization analysis, in conjunction with the results of limited scope performance tests conducted at the site, test the knowledge, skills, and abilities of the response forces, and help determine the effectiveness of the response forces against the DBT.

- **Step 9. Evaluate Physical Protection System Effectiveness and Estimate P_E.** The measure of overall PPS effectiveness is the probability of system effectiveness, P_E. System effectiveness is determined quantitatively using the following equation:
  - $P_E = P_I * P_N$

  where:
  - P_I = probability of interruption of the adversary attack by the response force (estimated in Step 7)
  - P_N = probability of neutralization of the adversary by the response force (estimated in Step 8)

  It is important to assess the entire PPS – not only the hardware, but also contingency plans, procedures, and possible variations in adversary attack scenarios. While previous sections have discussed timely detection, Probability of Interruption, and Probability of Neutralization as evaluation metrics, the security system must also perform against an array of possible attacks that may not be captured by path analysis techniques alone. Scenario analysis is an additional methodology used to further analyze system effectiveness, PE, by considering the effect of several alternative possible adversary attacks (scenarios) against the PPS.

- **Step 10. Identify Vulnerabilities and Areas for Improvement; and Propose Upgrades**. The assessment team reviews baseline system effectiveness and risk values and makes a determination of the effectiveness of the PPS elements in protecting targets against the DBT. If overall system effectiveness/risk meets the determined requirement, then the analysis is complete. Otherwise, system vulnerabilities are identified and areas for improvement are proposed. Both

improvements to the PPS functions (detection, delay, and response) and to the overall system are considered for increasing the system effectiveness (or reducing risk).

- **Step 11. Re-evaluate System with Proposed Improvements**. Once the upgrades are developed the system is analyzed with the postulated upgrades. The upgrade analysis is conducted and new estimates for probability of interruption, probability of neutralization, probability of system effectiveness, and risk are determined. The process is repeated until upgrades are identified that satisfactorily addresses system vulnerabilities and reduces the facility's overall risk to an acceptable level established by the government.

- **Step 12. Report Results and Recommendations**. The final step of the VA is reporting the results in a manner useable to the decision-makers responsible for PPS decisions. The reporting of results is typically conducted by two methods: briefings and written reports. The goal of the reporting phase is to provide accurate unbiased information that clearly and accurately defines the current system effectiveness of the evaluated PPS, estimates risks, and provides potential solutions if the current protection system is deemed ineffective.

Scenario Analysis

Scenarios Analysis requires more details about the attack and the defense. Evaluating neutralization (and overall effectiveness), in turn, requires more detail about how the adversary attack is conducted than just the path as the attack and site defenses must be simulated, using tabletop exercises, combat computer simulations, and/or Force-on-Force exercises.

While path analysis is most concerned with finding the most vulnerable path, scenario analysis is concerned with creating a 1) detailed representative set of adversary scenarios/attack plans, 2) detailed description of site security plans, procedures, and deployment conditions, and 3) performing a simulation of the interaction between adversaries and the PPS that is conducted as honestly and realistically as possible.

Thus, multiple timelines are needed, not just one as was the cased with path analysis. These scenarios should both be realistic for an adversary constrained within the Design Basis Threat and should cover the range of potential vulnerabilities seen in the PPS. While the quality of path analysis can drop when a vulnerable path is missed; the quality of scenario analysis can suffer both because vulnerabilities are overlooked in scenario formulation and because unrealistically effective scenarios are simulated against the PPS.

Comprehensive Scenario Analysis

In order to provide confidence that an analysis is comprehensive, it is necessary to follow a systematic, structured approach to identifying scenarios. The steps in one such approach are given below:

1. Identify the key questions to be addressed by the scenario analysis.
2. Identify major drivers of performance in the study and sort these drivers into those that are controllable within the study, such as the capability of the attacking force or security response options, versus those that are uncontrollable, such as the size of the DBT.
3. Collect necessary site data, including performance test data, timeline information from the path analysis, and detailed security plans and procedures.
4. Based on the information collected from steps 1-3, use either a formal approach to creating a set of scenarios using expert attack planners or an informal approach when such experts are not available. (This section will focus on how to accomplish the informal approach.)
5. Assess the system effectiveness, P_E, against the representative scenarios using either Subject Matter Experts (using criteria-based assessments) or one or more simulations – Tabletop analysis, computer simulations, or Force-on-Force exercises.
6. Document results and conclusions along with scenario descriptions

Evaluate Potential Design Basis Threat (DBT) Adversary Scenarios

These scenarios should both be realistic for an adversary constrained within the Design Basis Threat and should cover the range of potential vulnerabilities seen in the PPS. While the quality of path analysis can drop when a vulnerable path is missed, the quality of scenario analysis can suffer both because vulnerabilities are overlooked in scenario formulation and because unrealistically effective scenarios are simulated against the PPS.

Value of Using Expert Planners and Some Limitations

In a formal application of scenario analysis, one or more experienced attack planners should be used to develop the attack scenarios. Compared to others, such as engineers and security personnel, the expert planner can go a long way to keeping the scenario realistic. Personnel with many of the right skills can be found in military and similar organizations. One criterion for the expert to have is experience in planning missions with forces the size of the design basis threat. It is also important to find planners who appreciate that the adversary will typically carry out an attack lacking some of the capabilities that conventional militaries have. Without considering this limitation, the expert planner may develop plans that are fictitious: they appear to be possible for the threat to carry out but are not.

Scenario Development

When developing attack scenarios, they should challenge the plant security and operations to the maximum extent practicable within the constraints established by a DBT. The concept of the DBT is used to establish the expected threat to a facility. The DBT is used as a

management and design tool that helps facilitate informed decision-making and establishes technical requirements for security designers.

Thus, the scenarios selected should be those to which the Nuclear Power Plant (NPP) is judged to be most vulnerable. In a VA, the target set and sabotage scenario should be selected to exercise as many of the deficient aspects of the security program as practicable. Absent such an assessment, target set and scenario selection considerations would include the following:

- Minimization of the number of physical barriers that an adversary must overcome (e.g., selection of target sets with the minimal number of areas).
- Minimization of likelihood that adversary actions would be detected and correctly assessed.
- Minimization of likelihood of timely and effective security response

Identifying Site and Operational Vulnerabilities

In order to develop realistic scenarios, the adversary planners need to collect as much specific information regarding the site's PPS and operational state of the facility. There are three ways to collect this type of information:

1. Use passive insider information. A passive insider will pass on detailed information such as the specifics of the response force strategy, detailed blueprints of the facility that stores the target material, or specifics of the reactor that can make the target go critical. It is very important to put restrictions on the passive insider as to how much information is provided to the adversary; otherwise it can become unreasonable.

2. Conduct site surveillance. The adversary planners can collect valuable intelligence by going out to the site's PPS. They will go where they can't be detected to begin the surveillance. They are looking for guard/response force patterns. For example, every three hours a patrol vehicle patrols around the reactor building or every four hours a guard leaves the guard shack and enters the reactor building. Adversary planners also look for advantageous positions that will minimize detection and provide an element of surprise.

3. Adversary planners can utilize outside sources such as the World Wide Web, the Site's local Libraries, etc.

Identify operational vulnerabilities

In order to identify site vulnerabilities across various operational conditions and states, consider different:

- Operational conditions (operational versus non-operational)
- Target material configurations (reactor load-out versus operations)
- Response force alert levels and personnel "crews"
- Different upgrade packages

Exploiting the Vulnerabilities

When promising vulnerabilities have been identified, it will be required to develop an action plan how the each vulnerability will be exploited. The action plan will need to have the attention to detail and organization in how the attack will be executed. The following steps can be followed:

- First creating a list of essential tasks that have to be accomplished for the attack based on that vulnerability to succeed. Such a list might look like the following for a target:
    - Task 1: Enter building XYZ
    - Task 2: Collect 20 Kg of U235 in storage containers
    - Task 3: Leave site with material without pursuit by response forces
    - Task 4: Arrive undetected at safe house in city ABC
    - Task 5: Hold off responding units so that tasks 1 through 3 are accomplished

  These tasks should be kept as simple as possible.

- Next, creating sub-plans that describe how one or more teams of attackers can perform each task within resource constraints. These sub-plans should describe:
    - Who is involved?
    - What are they doing as a function of time?
    - How are they performing each step?
    - What equipment are they using?
    - How are they transporting the equipment?

- Finally, combine these sub-plans into a master attack plan/scenario description, adjusting sub-plans to meet overall constraints imposed by the DBT and perhaps the site as well as to achieve synchronization between teams.

Adding Supporting Team Sub-Plans to Scenarios

Supporting teams can be assigned to complete other essential tasks or to aid the main team directly. Often, the remaining tasks look like: "Hold off responding units so ..." or "Neutralize offsite response..." Thus, one good use of supporting teams is to delay or incapacitate the response through setting ambushes, creating diversions, and attempting to confuse the response.

Using Path Analysis for Scenario Development

Path analysis can suggest sub-plans that serve as the main or "direct" part of the attack (direct in the sense of going to the target). Such plans might be based on the minimum delay, minimum PI, or minimum PI*PN paths

Details can be added to these path descriptions to fill out the scenario. For example, instead of the step "Penetrate Fence" found in the path analysis, the scenario description might consist of: "Four adversaries bridge fence using ladder carried in from vehicle parked outside at night during a storm. Last adversary monitors radio traffic."

Of course, multiple scenarios can be developed for a single path by slightly varying the method by which the adversary attacks different protection elements along the path.

Be aware, though, the most-vulnerable path (MVP) from path analysis may be a poor basis for creating a scenario. This may occur because typically low PI paths should be corrected with upgrades during the path analysis phase. After such upgrades, the MVP should now have a high PI rendering that path less desirable At this stage scenario analysis might more profitably consider factors not found in path analysis: preventing neutralization and employing other teams to prevent interruption.

Insider Colluding With Outsider Adversary

It is important to recognize that one of the most damaging adversaries to a physical protection element is the insider. Therefore, an insider colluding with outsiders can be a formidable adversary. When determining the impact of a colluding insider on physical protection system effectiveness, consider the access, knowledge, and authority entrusted to the insider, and consider how these might be abused to:

- reduce the probability of detection of a sensor or procedure. *Example: the probability of covert/deceitful entry through an entry portal*
- reduce the delay time offered by barriers. *Example: anything with locks for which the adversary has key access*
- increase the time of response. *Examples: block response doors, disable vehicles, divert response teams, etc.*
- decrease the number of respondents. *Examples: detonate pre-positioned explosives, or divert part of the force to another incident.*

The importance of achieving synchronization

Lack of synchronization can result in failure of the attack due to earlier detection than planned or piecemeal attacks on targets. Achieving synchronization requires planning so that multiple teams can coordinate their progress at key steps (e.g., they all are in correct positions when detection occurs, task time estimates are reliable so that some teams don't fall behind others; and surprises (e.g., chance encounters with security or site personnel) are limited.

Complete Credibility Check

When reviewing potential scenarios, credibility and consistency are important considerations for a useful analysis. The credibility implies that although an adversary might be able to successfully perform one or two difficult tasks in a scenario, it would be incredible for him to perform a long series of them. For example, it might be credible for an adversary to employ a hot air balloon to cross a protected area perimeter. It might also be credible for him to rappel from the balloon basket onto the target building ceiling. It might also be credible for him to engage and kill a pair of well-trained guards using a hand gun. However, it would be incredible to propose that an adversary might employ the hot air balloon, rappel onto the building, and, simultaneously engage and neutralize two response force personnel using a handgun.

Defeat Methods in Scenario Should Be Consistent

Consistency implies that the defeat methods pursued along the scenario make sense. For example, it might be possible to consider that an adversary might drive a vehicle through a wall in order to penetrate a building quickly. It would also be credible for an adversary to employ a false badge to deceive a guard posted at a vital area entrance. It would not, however, be credible for the adversary to penetrate the building wall using a vehicle, and then produce a false badge for the guard at the vital area entrance.

Use of Scenarios with maximum equipment

The best scenario for the adversary does not always use all of the equipment allowed within the design basis threat. This may occur because not all of the equipment may provide an advantage to the attackers once training and the need to hide the attack from intelligence services is factored in. Adding equipment may also increase the complexity of the scenario, making it more risky.

Reasons why Scenarios may Fail

Attack scenarios can fail for other reasons than neutralization. Failure may occur due to early detection on the attack plan before that point that adversaries planned to be detected), due to detection by intelligence organizations directly or by populace during the lead-up to the attack. Non-combat failures can also lead to scenario failure due to a variety of reasons:

- inability to get weapons or equipment needed;
- Breakdowns of vehicles, communications equipment
- Exhaustion of team-members during the attack
- Tool/explosive failure to breach
- Timing and synchronization failures
- Wrong plan due to bad information
- Inadequate training and rehearsal

Physical Protection System (PPS) Effectiveness

Once a comprehensive set of credible scenarios has been developed using realistic assumptions about the system and adversary and the defeat strategies have been developed, the effectiveness of the physical protection system (PPS) effectiveness is typically determined by one or more simulations, either table-top, computer simulation, or Force-on-Force exercises. Probability of System Effectiveness, P_{EFF}, can either be determined by estimating P_{EFF} directly or by estimating Probability of Interruption and Probability of Neutralization separately and then using the formula: $P_I * P_N = P_{EFF}$.

Combining the Results of Different Simulations

When having a choice of simulations, the best sequence of use is shown below in Figure 21-4. Performance tests typically come first; provide necessary input to Table-tops. Table-top exercises can often foresee the analysis and logistic issues that will arise in computer simulations and FoF exercises. In some cases, issues are identified in table-tops that have to be addressed before other simulations can be performed.

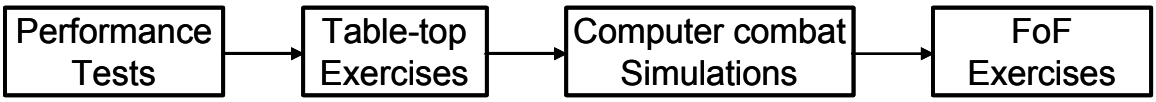

Figure 21-4: Proposed Sequence for Performing Neutralization tool: